Joining Consumer Sentinel

Consumer Sentinel is an investigative cyber tool and complaint database, restricted to law enforcement use, that provides thousands of civil and criminal enforcement agencies immediate and secure access to identity theft, internet, telemarketing (including do not call), and other consumer fraud-related complaints. The instructions below explain how your organization can become a Consumer Sentinel member and gain access to millions of consumer fraud and identity theft complaints accessible on the Consumer Sentinel restricted access web site.

1. Check the Members List on the Consumer Sentinel Public Web site (www.consumer.gov/sentinel/members.htm) to see if your law enforcement organization is already a Sentinel member. If your organization is already a member then skip to Step 3 to sign up for an individual account.

2. If you do not see your organization listed, your agency will need to execute the Consumer Sentinel Network Confidentiality Agreement. The Confidentiality Agreement is a three page, agency-to-agency agreement. The agreement defines the Consumer Sentinel access privileges and confidentiality rules. **The Consumer Sentinel Network Confidentiality Agreement must be signed by someone with the authority to sign for your entire organization.** Print the name of your organization in the space provided at the top of page one and on page three. Only one confidentiality agreement is required per organization.

3. Each individual Consumer Sentinel user needs to complete the one page application for access to the Consumer Sentinel web site. The information on the application is used to create a unique account for each individual Sentinel user. As opposed to the Confidentiality Agreement, the individual user's direct supervisor can sign the individual applications as the approving official. Remember to include your email address and your approving official's signature.

   Fax the Confidentiality Agreement and all individual Applications for Access to the Consumer Sentinel team at 202-326-3392. Address them to the Consumer Sentinel Program Manager.

4. Upon receipt of the executed Confidentiality Agreement and individual applications, the Sentinel staff will create an agency account and process the individual applications. Within three to four weeks, individual users who completed an application should receive two packages in the mail from us with log on instructions and password information.

If you have any questions, please contact us at 877-701-9595 or by email at sentinel@ftc.gov.

Consumer Sentinel Sign-Up Checklist

____ 1. Agency's Name on Confidentiality Agreement (pages 1 and 3).

____ 2. Confidentiality Agreement executed by someone with authority to sign for entire agency.

____ 3. Individual application for access completed by all users requiring access to Sentinel.

____ 4. All individual applications include e-mail address and approving official's signature.

____ 5. All paperwork faxed to Sentinel staff at 202-326-3392.

Consumer Sentinel Network Confidentiality Agreement

This agreement is entered into between the Bureau of Consumer Protection ("Bureau") of the Federal Trade Commission ("FTC") and the _____, in conjunction with all other domestic and foreign agencies and other entities similarly agreeing. The purpose of this agreement is to facilitate the confidential exchange of consumer complaint information, including information about consumer fraud and deception perpetrated through the Internet, direct mail, telemarketing, or other media, under the conditions set forth below.

The Consumer Sentinel Network

1. The FTC, in conjunction with the National Association of Attorneys General, Canshare, and PhoneBusters, has developed the Consumer Sentinel--an automated database to store investigatory information provided by participating law enforcement agencies and other contributors about consumer fraud and deception. Pursuant to the Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. §1028, the FTC also has developed the Identity Theft Data Clearinghouse--an automated database to store investigatory information provided by consumers, participating law enforcement agencies, and other contributors about identity theft. The FTC makes information contained in the Consumer Sentinel and the Identity Theft Data Clearinghouse available through the Consumer Sentinel Network. The information contained in both databases is known collectively as "Consumer Sentinel Network" information. This information exchange program is consistent with Section 6 (f) of the Federal Trade Commission Act, 15 U.S.C. § 46(f), Commission Rules 4.6, 4.10, and 4.11(c) and (d), 16 C.F.R. §§ 4.6, 4.10, and 4.11(c) and (d) (2000), and the Privacy Act of 1974, as amended, 5 U.S.C. § 552a. See also 57 FR 45678, 45700 (1992); 64 FR 57887 (1999) (FTC Privacy Act system notices for consumer complaint system generally and identity theft complaint system specifically, specifying routine uses of system records).

2. The information contained in the Consumer Sentinel Network does not include confidential commercial material, but is limited to information derived primarily from consumer complaints and other information gathered during identity theft, fraud, and other consumer protection investigations. This information may include, among other things, the names of companies and company representatives; the identity of the products or services involved; the status of ongoing law enforcement actions; and the names and telephone numbers of assigned staff.

Data Contribution from Participants

3. The signing entities and other data contributors may enter relevant information into one or both databases through the use of computer terminals located in their offices or by providing such information to other participants who will input such data into the system. Where necessary, the FTC subsequently loads this information into the automated databases, which are controlled by the FTC.

Access to Consumer Sentinel Network Information

4. Information in the Consumer Sentinel Network shall be made available as follows:

   a. Information in the Consumer Sentinel database will be available only to the FTC and participating domestic and foreign law enforcement agencies that sign a Consumer Sentinel Network confidentiality agreement. The form, substance and extent of disclosures to foreign law enforcement agencies shall be within the discretion of the FTC, subject to mutual agreement between the FTC and the foreign law enforcement agency.

   b. Information in the Identity Theft Data Clearinghouse will be made available to the FTC and participating domestic and foreign law enforcement agencies that sign a Consumer Sentinel Network confidentiality agreement. The form, substance and extent of disclosures to foreign law enforcement agencies shall be within the discretion of the FTC, subject to mutual agreement between the FTC and the foreign law enforcement agency. Limited information from the Identity

Theft Data Clearinghouse also will be available to other participating domestic government agencies, consumer reporting agencies, and private entities that sign this agreement, to the extent consistent with the Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. §1028, and the Privacy Act, 5 U.S.C. 552a. The form and substance of disclosures to other participating domestic government agencies, consumer reporting agencies, and private entity participants is at the discretion of the FTC.

Confidentiality and Use of Consumer Sentinel Network Information

5. All parties participating in this information exchange system do so with the understanding that all Consumer Sentinel Network information, including all information available on the Consumer Sentinel Network's restricted website, will be kept confidential. In particular, the party signing this agreement agrees not to release such information to anyone other than its employees, consultants and contractors, or bona fide law enforcement agency personnel who are bound by this agreement and have a need to know such information. The FTC reserves the right to limit or revoke access to such information by any participating agency or other entity that breaches any of the terms of this agreement.

6. The party signing this agreement agrees to use information contained in the Consumer Sentinel Network in the manner indicated below (check only one designation):

a. _____ The party signing this agreement is a domestic or foreign law enforcement agency and agrees to use the Consumer Sentinel Network information to which it has access under paragraph 4 of this agreement only in connection with law enforcement purposes.

OR

b. _____ The party signing this agreement is a participating domestic government agency, consumer reporting agency, or private entity, and agrees to use the limited Identity Theft Data Clearinghouse information disclosed to it only to prevent or investigate frauds described in 18 U.S.C. § 1028 (a), subject to such additional conditions as designated by the FTC.

7. Except as authorized by law, the Bureau agrees that information contained in the Consumer Sentinel Network will not be released to anyone other than participating agencies and other entities as delineated in this agreement, and to employees of and consultants and contractors of such entities and of the FTC with a need to know such information. Should the FTC receive an official request from another federal law enforcement agency or from Congress[1] or should the FTC be directed to furnish information in the Consumer Sentinel Network to a nonparticipant by a court with jurisdiction to issue such an order, however, the FTC may, in its discretion, furnish that information subject to applicable statutory restrictions and in a manner consistent with the need to preserve the confidentiality of that information. In addition, the FTC will make aggregate statistics available to participants upon request and will continue to release trend data to the general public.

8. The signing party agrees that, should it receive a request for access to this material or should that information become subject to compulsory process, it will immediately notify the FTC contact person of these facts so that a timely decision can be made on whether to furnish the requested information and, if the information is to be furnished, how to furnish it in a manner that will preserve its confidentiality.

9. The FTC has appointed the Associate Director for Planning and Information, Bureau of Consumer Protection, to be its contact person for purposes of this information exchange program with respect to domestic agencies and other entities. This official is responsible for ensuring the confidentiality of the

[1] It is the FTC's policy to provide information to Congress upon official request, although the Federal Trade Commission will request that the confidentiality of the information be maintained.

information contained in the Consumer Sentinel Network and, in appropriate circumstances, for authorizing participants to make further disclosures of the material in response to requests for access or compulsory process. The Associate Director has also been delegated authority from the Commission to respond to requests for access from domestic law enforcement agencies to any FTC documentary materials relating to consumer fraud. Such requests will be handled under the procedures set forth in Commission Rule 4.11(c), 16 C.F.R. § 4.11(c), whereby the requesting party must submit a certification that the material will be used for law enforcement purposes and be kept confidential. The Commission has delegated to the Director, Office of International Affairs, the authority to execute Consumer Sentinel Network confidentiality agreements with any foreign law enforcement agency whose access has been authorized or is authorized in the future by the Commission or by the Commission's delegate. The Commission has also delegated to the Director, Office of International Affairs, authority to disclose certain nonpublic information to foreign law enforcement agencies. Such execution of confidentiality agreements with foreign law enforcement agencies and such disclosure to foreign law enforcement agencies shall be pursuant to 67 FR 45738 (2002) or other Federal Register notices or rules published by the Commission. The Director of the Bureau of Consumer Protection, subject to redelegation, may also respond to foreign access requests for certain information on consumer protection pursuant to the delegation authority set forth at 62 Fed. Reg. 15185 (1997).

The_____agrees to the above conditions.

Signature _____

Name _____

Title _____

Dated _____

Mailing Address _____

_____

Phone Number _____

Email Address _____

_____
David M. Torok
Associate Director, Division of Planning and Information
for the Bureau of Consumer Protection

Dated _____

_____
Randolph W. Tritell
Director, Office of International Affairs,
for the Federal Trade Commission

Dated _____

Application for Access to the Consumer Sentinel Network

PRINT LEGIBLY

The absence of any requested information will delay the processing of your application.
If you have any questions, please contact Consumer Sentinel Support at sentinel@ftc.gov or 877-701-9595.

APPLICANT IDENTIFICATION

Applicant's Name (Last, First, Middle Initial)		Fax Number (include country code if outside US or Can)
Applicant's Title	Telephone Number (include country code if outside US or Canada)	E-mail Address
Agency Name (and country, if outside US)	Organization Code ***(completed by FTC)***	Web browser (circle one) **IE** or **Netscape** **Version:**
Mailing Address		

CERTIFICATION

I have reviewed the Terms of Use and the Consumer Sentinel Network Confidentiality Agreement (CA) (**http://www.ftc.gov/sentinel/cs_signup.pdf**). I understand that the Consumer Sentinel Network contains sensitive personally identifiable information and sensitive health information. In using the Consumer Sentinel Network, I agree to abide by the applicable guidelines in the Terms of Use and the CA. I also certify that I will use the Consumer Sentinel Network only for approved law enforcement purposes. I understand that use for any other purpose, including unauthorized access or disclosure, may constitute a violation of Section 10 of the FTC Act and the CA.

Signature of Applicant	Date

THE FOLLOWING MUST BE COMPLETED BY APPLICANT'S AGENCY.

Signature of Approving Official from Applicant's Agency	Date

Approving Official's Name	Title of Approving Official
Fax to: **202-326-3392**	**OR** Mail Original To: Consumer Sentinel Project Team, Federal Trade Commission, 600 Pennsylvania Ave., NW H-228, Washington, DC 20580

For FTC Use Only

BCP Approval			Date
CA	V or S	Signature	Date

Consumer Sentinel Network
Terms of Use

The Consumer Sentinel Network Confidentiality Agreement signed by your agency and the user application signed by you require you to treat information in Consumer Sentinel in a confidential manner. Information in consumer Sentinel includes, but is not limited to, complaints, alerts, top violator and other reports, and reference materials. Information in Consumer Sentinel must not be made public or shared with non-Sentinel member agencies. This rule extends even to acknowledging the existence of complaints against a particular subject. Further, the information must be used only for law enforcement purposes. If you are compelled to disclose Sentinel data, please contact the Sentinel team immediately so that we can determine if you can release the data and, if so, how to furnish it in a way to protect its confidentiality.

It is worth remembering that Consumer Sentinel contains personally identifiable information about consumers and identity theft victims, as well as individual subjects. Although we do not ask for it, consumers sometimes provide highly sensitive information about bank accounts, credit cards, their medical history, Social Security numbers, etc. in the comments field. We cannot review every complaint to redact this information. Instead, we rely on you to keep it confidential. Even a consumer's name and phone number, in conjunction with other information, can be used by fraudsters and identity thieves.

Below are requirements to protect Sentinel data. You must follow these security measures to ensure compliance with the Confidentiality Agreement and your user agreement.

- Do not export your VeriSign digital certificate (for which you will need to register and download after the Federal Trade Commission has processed your application) to other users in your agency. If other users are having problems accessing Consumer Sentinel, please have them call the Sentinel support line, or you can conduct searches on their behalf.

- Ensure that when you register for your VeriSign digital certificate, you set the security level to "**High**."

- If your certificate security level is set to "**High**," you will be prompted for a password. Ensure that this password is different from your Consumer Sentinel Network log in password. Also, do not share your certificate password with anyone.

- Do not share your Consumer Sentinel Network log in user ID and password with anyone. Do not set your computer/browser to "remember" your user ID and password. If you keep a hard copy of your user ID and password, ensure that it is in a safe place (preferably under lock and key).

- Only access the Consumer Sentinel Network from your work computer. In addition to a firewall, it would be beneficial if your work network or computer has anti-virus and anti-spyware programs, and that they are updated automatically (if you are unsure, ask your network administrator).

- Up-to-date security patches for your operating system and browser must be installed on your computer. Also determine if you are using the most recent version of the browser.

- Do **NOT** save Consumer Sentinel Network data locally (i.e., your computer, agency network file share, CD's, disks, DVD's, etc.). In other words, do not use the "Save As" feature in your web browser, capture screen shots of Sentinel pages, or copy and paste data from Sentinel to other programs (e.g., Excel or Access).

- If you must save Sentinel data for a law enforcement purpose, then use some form of electronic encryption to protect the data. You can use programs such as PKZIP or WinZip to encrypt these files. Ensure that you use a strong password with at least eight (8) characters, and the algorithm is set to AES (256-bit).

- If you must save Sentinel data, delete it as soon as possible. In doing so, remember to delete the file(s) from your "recycle bin;" otherwise, it stays on your computer. In the case of removable media (e.g., CD's or disks), ensure that you either delete the file entirely or destroy the media completely.

- Any saved Sentinel data **MUST** be deleted within 90 days after being saved or extracted. This includes Consumer Sentinel Network data that has been inserted in a spreadsheet or another database.

- If possible, do **NOT** print complaints, alerts or any other information from the Consumer Sentinel Network. If you must do so, then keep the hard copies under lock and key. As with saved data, all printed Sentinel information **MUST** be destroyed (i.e., shredded) within 90 days after printing.

- Log out of Sentinel when you are finished using it. In addition, do not leave an open session running on an unattended and unlocked computer.

Your continued use of the Consumer Sentinel Network will constitute your agreement to be bound by these terms and conditions.